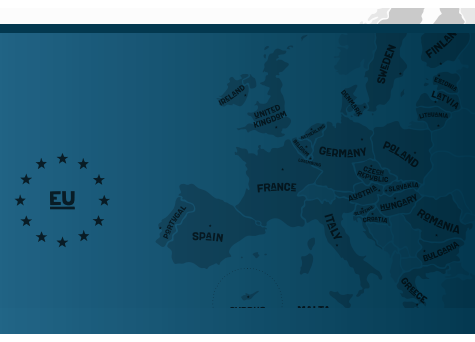
LogMeIn Rescue and the GDPR



On May 25, 2018, the European Commission will require all global organizations conducting business in the European Union (EU), as well as businesses maintaining or processing EU personal data, to comply with the General Data Protection Regulation (GDPR). These new rules aim to provide EU citizens with greater control over how their personal data is collected, stored, transferred and used, while also simplifying the regulatory environment across the EU.

LogMeIn Rescue's compliance with GDPR

As a global company with customers in nearly every country in the world, LogMeIn has always made it a priority to protect the personal data of our customers and their end users. GDPR represents an opportunity to continue our commitment in this area. LogMeIn (including LogMeIn Rescue) already participates in the EU-U.S. and Swiss Privacy Shield Frameworks and is compliant with current applicable EU data protection rules. At LogMeIn, our ongoing compliance review and actions build on our existing investments in privacy, security and the operational processes necessary to meet the applicable requirements of GDPR by May 25, 2018.

To make sure that customers understand LogMeIn's general philosophy towards GDPR, our goals by the date it will be enforced and how they may be able to use Rescue in a GDPR-compliant way, it is important to remember a few points:

- In GDPR terminology, Rescue is a "Data Processor" and you, our customer, are the "Data Controller" for all Customer Content (as defined in the Terms of Service). This means that you are in charge of determining the fate of all data uploaded by you or users on your account. Rescue will comply with your instructions and the terms of any written agreement or contract as to how to deal with data (within the capabilities of the product).
- As Data Controller, you also own the relationship directly with users in your account – these users are considered to be "Data Subjects" under the GDPR. Data Subjects have certain rights under the law and Rescue provides tools for you to assist Data Subjects in the exercise of their rights.
- For your privacy and security, we will delete your Content (i) at your request or (ii) after your account is no longer provided under a paid subscription.
- At any time, you have the right and the necessary tools to get your content out of Rescue. We make it easy for you to maintain your own local backup copy.

It is very important to remember that by using Rescue you are not necessarily or automatically fully GDPR compliant. We encourage you to verify that you meet all applicable aspects of the regulations and to seek legal advice, if needed.

Increasing your GDPR compliance with Rescue

As noted above, LogMeIn is well on its way to GDPR compliance and we believe that Rescue may be able to assist our customers in their compliance efforts by leveraging the following functionality:

- **Security:** Rescue employs the same security levels used and trusted by major banking institutions with TLS 1.2 transport security with AES 256-bit encryption, as well as two-step verification logins.
- **Data storage:** Chat logs and custom fields are secured with AES 256-bit encryption and the Rescue database is backed up automatically every 24 hours. The backup database is stored in the data center with the same encryption as the original.
- **Data residency:** Rescue's Data Residency option allows new customers to choose where to store content, either in Europe or in the U.S. Once you've chosen a data residency location, your content will be hosted and stored from that specific region.
- **Data deletion:** Rescue allows customers to export their Content and delete their account, if required. This feature may allow a customer to meet requirements around deletion of personal data after its intended use is complete, consent is withdrawn or if a legitimate business purpose no longer exists.

The bottom line of GDPR? It's all about ensuring data subjects' privacy and providing for the appropriate handling of personal data. We believe that if our customers are ever called upon to demonstrate their GDPR compliance (perhaps, for example, during an audit), the following Rescue features may be able to help:

- **Permission-based security:** Get permission from end users before using each Rescue function, including Remote Control, Desktop View, File Transfer, System Information and Reboot & Reconnect.
- **Administration Center:** Centrally perform management tasks such as creating and assigning permissions for other administrators, technicians and groups or create and view reports.
- **Session reporting and recording:** Securely manage your help desk by defining permissions for Technician Groups, view details of technician activity and audit session activity through detailed logging.
- **Auditing and logging:** A remote support solution must place strong emphasis on accountability. LogMeIn Rescue provides two distinct auditing features. First, the "Chat log" is saved in the Rescue database. The Chat log contains events and chat messages such as session start and end time and if a file was transferred during the session. Second, session recording allows the entire session to be recorded in a video format and may be important for internal compliance purposes.

Learn more about LogMeIn's GDPR compliance, including product-specific Security and Privacy Operational Controls (SPOCs), at logmeininc.com/gdpr.